Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Groups of Transformations of Sylow Subgroups.

By G. A. Miller.

§ 1. *Introduction.*

The first part of the present paper is devoted to a study of some of the properties of a transitive substitution group which is a group of transformations of Sylow subgroups. In particular, we shall prove the following theorem: *If the Sylow subgroups of order* p^m *in any group* (G) *are transformed according to an imprimitive substitution group, the number of these subgroups must be of the form* $(1+k_1p^\alpha)(1+k_2p^\alpha)$, *where each of the two numbers* k_1, k_2 *exceeds zero and* α *is determined by the fact that the largest number of common operators in any two such Sylow subgroups of* G *is* $p^{m-\alpha}$. It is evident that α can not be less than unity nor greater than m.

In the second part of the paper we determine some properties of the groups which involve certain given numbers of Sylow subgroups. In particular, we prove that if a group G contains exactly three Sylow subgroups, these subgroups must generate a group of order $3 \cdot 2^m$, and this group is a characteristic subgroup of G if it does not coincide with G; if G contains exactly four Sylow subgroups, these subgroups generate a group whose order is either $12 \cdot 3^{m-1}$ or $24 \cdot 3^{m-1}$, and this group is again either G itself or a characteristic subgroup of G. A somewhat similar theorem is proved as regards groups containing exactly six Sylow subgroups.

The $1+kp$ Sylow subgroups of order p^m in G are transformed according to a transitive substitution group (K) of degree $1+kp$ which has an $(1,\alpha)$-isomorphism with G. The invariant subgroup (H) of G which corresponds to the identity in K involves only one Sylow subgroup of order p^{α_1}, since the operators of H whose orders are powers of p must be contained in every Sylow subgroup of G. To every Sylow subgroup of G there corresponds one and only one Sylow subgroup of K, and hence G transforms its $1+kp$ Sylow subgroups of order p^m in exactly the same manner as K transforms its $1+kp$ Sylow subgroups of order p^β, $\beta \overline{\gtrless} m$. That is, the letters of the substitutions of K may stand for the various Sylow subgroups of order p^β in K.

The subgroup (K_1) of K which is composed of all its substitutions omitting one letter involves one and only one Sylow subgroup of order p^β and of degree kp. Moreover, if any transitive group has the property that its subgroup composed of all the substitutions which omit a given letter involves one and only one Sylow subgroup of degree one less than the degree of the group, it evidently permutes these Sylow subgroups in the same manner as it permutes its own letters.* Hence the theorem: *The necessary and sufficient condition that a transitive group of degree n is a group of transformations of Sylow subgroups is that its subgroup composed of all its substitutions which omit a given letter involves one and only one Sylow subgroup of degree* $n-1$.

From this theorem it follows directly that the only symmetric groups which are groups of transformations of Sylow subgroups are those of degrees 3 and 4, and the only alternating groups having this property are those of degrees 4 and 5. The symmetric group of degree 3 is clearly the only group of this degree which can be a group of transformations of Sylow subgroups, while the alternating and the symmetric group of degree 4 are the only two groups of degree 4 which have this property. There are three groups of degree 5 which are groups of transformations of Sylow subgroups; viz., one of each of the orders 10, 20, 60. Only two of the sixteen transitive groups of degree 6 are groups of transformations of Sylow subgroups; viz., the two groups of orders 60 and 120 respectively.

Since K_1 is of degree kp, it follows directly that a group of transformations of Sylow subgroups can not involve any invariant operator besides the identity.† From this fact and the elementary observations of the preceding paragraph it results that a large number of transitive substitution groups can not be groups of transformations of Sylow subgroups. In particular, it has been seen that no imprimitive group whose degree is less than eight can be such a group of transformations. We proceed to consider some of the properties of imprimitive groups which are also groups of transformations of Sylow subgroups.

§ 2. *Imprimitive Groups of Transformations of Sylow Subgroups.*

Suppose that K is imprimitive. All the substitutions of K_1 must transform at least one system of imprimitivity of K into itself. The number of letters in this system must be one more than the letters in one or more of the transitive constituents of K_1. Since each of these transitive constituents involves an invariant subgroup of order p^λ, $\lambda > 0$, it results that the degree of each of these constituents is divisible by p. In fact, if no two of the $1 + kp$ Sylow subgroups of G have more than $p^{m-\alpha}$ common operators, each of these transitive constituents is divisible by p^α, and hence the number of letters in a system of imprimitivity of G is of the form $1 + k_1 p^\alpha$.

---

* *Bulletin of the American Mathematical Society*, Vol. II (1896), p. 145.

† Kuhn, AMERICAN JOURNAL OF MATHEMATICS, Vol. XXVI (1904), p. 67.

Since the degree of K is divisible by $1 + k_1 p^\alpha$, it is necessary that the total number of letters in K is of the form $1 + k_1 p^\alpha + k_0 p^\alpha$, where k_0 is divisible by $1 + k_1 p^\alpha$, and hence the degree of K is $(1 + k_1 p^\alpha)(1 + k_2 p^\alpha)$, where each of the numbers k_1, k_2 exceeds 0. As K is any group of transformations of Sylow subgroups, we have proved the following theorem: *If the Sylow subgroups of order* p^m *in a group are transformed under this group according to an imprimitive substitution group, the number of these Sylow subgroups is of the form* $(1 + k_1 p^\alpha)(1 + k_2 p^\alpha)$, *where none of the integers* k_1, k_2, α *is zero.* The value of α may be determined by the fact that two of these Sylow subgroups have at most $p^{m-\alpha}$ operators in common.

When $p = 2$, the theorem of the preceding paragraph does not yield any information, since every odd composite number can be represented in the form $(1 + 2k_1)(1 + 2k_2)$, where each of the numbers k_1, k_2 exceeds 0. Moreover, the dihedral group of order $2(1 + 2k_1)(1 + 2k_2)$ transforms its Sylow subgroups of order 2 according to an imprimitive group, k_1 and k_2 being any integers exceeding zero. It follows directly from the preceding theorem that 9 is the lowest degree for which imprimitive groups of transformations of Sylow subgroups exist, and it is not difficult to verify that there are exactly five groups of this degree which are imprimitive groups of transformations of Sylow subgroups; viz., two of order 18, one of order 36 and two of order 54.

Since the Sylow subgroups of order p^β in K generate a transitive group, it results that the operators in K_1 whose orders are powers of p must permute a multiple of p systems of imprimitivity of K. That is, the transitive group of degree $1 + k_2 p^\alpha$ according to which the systems of imprimitivity of K are transformed is non-regular and involves substitutions of degree lp. In particular, not only must the Sylow subgroups always be transformed according to a non-regular group, but when these subgroups are transformed according to an imprimitive group these systems of imprimitivity must also be transformed according to a non-regular transitive group.

§ 3. *Groups Involving a Small Number of Sylow Subgroups of the Same Order.*

The smallest number of non-invariant Sylow subgroups of the same order in any group is evidently three, and if a group G contains exactly three Sylow subgroups of the same order this order is 2^m, and the operators of G transform these subgroups according to the symmetric group of order 6. To the identity of this symmetric group there corresponds a subgroup H of G which involves a characteristic subgroup of order 2^{m-1}. The subgroup of G which is generated by the three Sylow subgroups of order 2^m contains this characteristic subgroup, and the corresponding quotient group is generated by two operators of order 2. Hence this quotient group is dihedral and, as it involves only three operators of order 2, it must be the symmetric group of order 6. This proves the theorem: *If a group G involves exactly three Sylow subgroups of order 2^m, these subgroups generate a group of order $3 \,.\, 2^m$.* This group is evidently a characteristic subgroup of G if it does not coincide with G.

Suppose that G involves four Sylow subgroups of order 3^m and is generated by them. These four subgroups are transformed under G according to the alternating group of degree 4, since a group which contains a subgroup of half its order can not be generated by operators of odd order. The invariant subgroup H of G which corresponds to the identity in this alternating group involves a characteristic subgroup of order 3^{m-1}, and the corresponding quotient group (G') is generated by two operators (s_1, s_2) of order 3, and we may suppose that these operators correspond to the cycles abc, abd in the given alternating group.

Since $(s_1 s_2)^2$ is invariant under G', it results that $s_1 s_2$, $s_2 s_1$ are two operators which have a common square, and hence the product of one of these operators into the inverse of the other is transformed into its inverse by each of them. By means of this property it is easy to find an upper limit for the order of this product as follows:

$$(s_1 s_2 s_1^{-1} s_2^{-1})^2 = s_1 s_2 s_1^2 s_2^2 s_1 s_2 s_1^2 s_2^2 = (s_2 s_1)^2 s_1 s_2 s_1^2 s_2 s_1 s_2^2 = (s_1 s_2)^6.$$

Since $(s_1 s_2)^6$ is both invariant under K and also transformed into its inverse by $s_1 s_2$, it results that its order is a divisor of 12. This order can however not be divisible by 3, and hence it must divide 4. If $s_1 s_2$ is of order 2, it is clear that K is the tetrahedral group, as it is generated by two operators of order 3 whose product is of order 2. On the other hand, if $s_1 s_2$ is of order 4, the two operators $s_1 s_2$, $s_2 s_1$ must generate the quaternion group, since they have a common square and

$$(s_1 s_2)^{-1} s_2 s_1 \,.\, s_1 s_2 = s_2^2 s_1^2 s_2 s_1^2 s_2 = (s_2 s_1)^2 s_2^2 s_1 \,.\, s_2^2 s_1^2 s_1^2 s_2 = (s_2 s_1)^3,$$

since $s_1 s_2 = s_2^2 s_1^2 (s_2 s_1)^2$, and $(s_2 s_1)^2$ is invariant under G'. This quaternion group is invariant under G', since $s_1^2 s_2 s_1^2 = (s_2 s_1)^2 s_1 s_2^2 s_1 = (s_2 s_1)^2 \,.\, s_1 s_2 \,.\, s_2 s_1$. Hence

$\{s_1, s_2\}$ is the group of order 24 which does not involve a subgroup of order 12 whenever $s_1 s_2$ is of order 4.

These results establish the theorem: *If a group contains exactly four Sylow subgroups of the same order, they generate a group whose order is either* $4 . 3^m$ *or* $8 . 3^m$, *and the quotient group with respect to the* 3^{m-1} *common operators is either the tetrahedral group or the non-twelve group of order* 24. If the order of the entire group exceeds the order of the group generated by these Sylow subgroups, the latter group is clearly a characteristic subgroup of the former.

If G contains exactly six Sylow subgroups of order 5^m and is generated by these subgroups, it must transform them according to the primitive group of degree 6 and order 60. Hence G is isomorphic with the alternating group of degree 5. We shall first assume that $m=1$ and that G is generated by the two operators s_1, s_2 which correspond to *abcde* and *aebcd* respectively of the isomorphic alternating group. Hence $s_1 s_2$ corresponds to the substitution of order 2, *ac . bd*. We shall prove that the order of $s_1 s_2$ is either 2 or 4. It is clear that the operators of G which correspond to the identity in the alternating group of order 60 constitute the central of G; and we shall prove that the order of this central is either 1 or 2, and hence the order of G is either 60 or 120.

Since $s_1 s_2$, $s_2 s_1$ have their squares in the central of G and are conjugate under G, they must have a common square, and hence the product of one of these operators into the square of the other is transformed into its inverse by each of them. By means of this property we obtain an upper limit for the order of one of the invariant operators of G as follows:

$$(s_1 s_2 s_1^4 s_2^4)^3 = s_1 s_2 s_1^4 s_2^4 s_1 s_2 s_1^4 s_2^4 s_1 s_2 s_1^4 s_2^4 = (s_1 s_2)^5 s_1^4 s_2^3 s_1^3 s_2^3 s_1^3 s_2^4 = (s_1 s_2)^6 (s_1^3 s_2^3)^3.$$

As $s_1^3 s_2^3$ corresponds to *abd*, and hence $(s_1^3 s_2^3)^3$ is in the central of G, it results that $(s_1 s_2)^6 (s_1^3 s_2^3)^3$ is invariant under G. It is also transformed into its inverse by $s_1 s_2$, and hence its order is 1 or 2. That is, $(s_1 s_2)^{12} = (s_2^2 s_1^2)^6$.

On the other hand, $s_1^3 s_2^2$ corresponds to *ae . bc*, and hence $(s_1^3 s_2^2)^2 = (s_2^2 s_1^3)^2$. Proceeding as above we obtain

$$\begin{aligned}(s_1^3 s_2^2 s_1^2 s_2^3)^3 &= s_1^3 s_2^2 s_1^2 s_2^3 s_1^3 s_2^2 s_1^2 s_2^3 s_1^3 s_2^2 s_1^2 s_2^3 = (s_1^2 s_2^2)^9 s_1 s_2^3 s_1^3 s_2 s_1 s_2^3 s_1^3 s_2 s_1 s_2^3 s_1^3 s_2 \\ &= (s_1^2 s_2^2)^9 (s_1 s_2)^5 (s_2^2 s_1^2)^3 s_1 s_2 = (s_1^2 s_2^2)^{12} (s_1 s_2)^6.\end{aligned}$$

From these equations it results that $(s_1 s_2)^{12} = (s_1^2 s_2^2)^{-24}$. Combining this with the earlier result, it follows that $(s_1^2 s_2^2)^{30} = 1$. As the order of $s_1^2 s_2^2$ can not be divisible by 5, it results that $(s_1^2 s_2^2)^6 = 1$ and hence $(s_1 s_2)^{12} = 1$.

It is evident that $(s_1 s_2)^2 = (s_1^4 s_2 s_1^2)^2$ and hence

$$\begin{aligned}(s_1 s_2 s_1^3 s_2^4 s_1)^5 &= s_1 s_2 s_1^3 s_2^4 s_1^2 s_2 s_1^3 s_2^4 s_1^2 s_2 s_1^3 s_2^4 s_1^2 s_2 s_1^3 s_2^4 s_1^2 s_2 s_1^3 s_2^4 s_1 \\ &= (s_1 s_2)^9 s_1^3 s_2^4 s_1 s_2^4 s_1^2 s_2^4 s_1 s_2^4 s_1^2 s_2^4 s_1 s_2^4 s_1^2 s_2^4 s_1 s_2^4 s_1^2 s_2^4 s_1 \\ &= (s_1^2 s_2^3)^8 (s_1 s_2)^9 s_1^3 s_2^4 s_1 s_2 s_1^3 s_2 s_1 s_2 s_1^3 s_2 s_1 s_2 s_1^3 s_2 s_1 s_2 s_1^3 s_2 s_1 \\ &= (s_1^2 s_2^3)^8 (s_1 s_2)^{17} s_1^3 s_2^3 s_1^3 s_2 s_1 = (s_1^2 s_2^3)^8 (s_1 s_2)^{19} s_1^3 s_2^3 s_1^2 s_2^4 \\ &= (s_1^2 s_2^3)^{10} (s_1 s_2)^{19} s_1^3 . s_1^3 s_2^2 . s_2^4 = (s_1^2 s_2^3)^{10} (s_1 s_2)^{20}.\end{aligned}$$

From these equations it results that $(s_1 s_2)^{40} = (s_2^2 s_1^3)^{20}$, or $(s_1 s_2)^4 = (s_2^2 s_1^3)^{20}$, since $(s_1 s_2)^{12} = 1$.

As $(s_1 s_2)^2 = (s_2^3 s_1 s_2^3)^2$, we obtain in a similar manner the following equations:

$$\begin{aligned}(s_1 s_2^3 s_1^4 s_2^2)^5 &= s_1 s_2^3 s_1^4 s_2^2 s_1 s_2^3 s_1^4 s_2^2 s_1 s_2^3 s_1^4 s_2^2 s_1 s_2^3 s_1^4 s_2^2 s_1 s_2^3 s_1^4 s_2^2 \\ &= (s_1 s_2)^9 s_2^2 s_1^4 s_2 s_1^4 s_2^2 s_1^4 s_2 s_1^4 s_2^2 s_1^4 s_2 s_1^4 s_2^2 s_1^4 s_2 s_1^4 s_2^2 s_1^4 s_2^2 \\ &= (s_2^2 s_1^3)^8 (s_1 s_2)^9 s_2^2 s_1^4 s_2 s_1 s_2^3 s_1 s_2 s_1 s_2^3 s_1 s_2 s_1 s_2^3 s_1 s_2 s_1 s_2^3 s_1 s_2^2 \\ &= (s_2^2 s_1^3)^8 (s_1 s_2)^{17} s_2^2 s_1^3 s_2^3 s_1 s_2^2 = (s_2^2 s_1^3)^{10} (s_1 s_2)^{20}.\end{aligned}$$

From these equations it follows directly that $(s_1 s_2)^{40} = (s_2^2 s_1^3)^{-20}$, and if we combine this with the result of the preceding paragraph, we have that $(s_2^2 s_1^3)^{40} = 1$. Since the order of $s_2^2 s_1^3$ is not divisible by 5, it results that $(s_2^2 s_1^3)^8 = 1$, and hence $(s_1 s_2)^{80} = 1$. If the last equation be combined with $(s_1 s_2)^{12} = 1$, it results that $(s_1 s_2)^4 = 1 = (s_1^2 s_2^3)^4 = (s_2^2 s_1^3)^4$.

Since

$$\begin{aligned}(s_2^2 s_1^3)^2 &= s_2^2 s_1^3 s_2^2 s_1^3 = s_2^2 s_1^2 . s_1 s_2 . s_2 s_1 . s_1^2 = s_2^2 s_1^2 s_2^4 s_1^3 s_2^4 s_1^2 \\ &= s_2^2 s_1^2 s_2^2 . s_2^2 s_1^3 . s_2^4 s_1^2 = s_2^2 s_1^2 s_2^2 s_1^2 s_2^2 s_1^2 (s_2^2 s_1^3)^2,\end{aligned}$$

it results that $(s_1^2 s_2^2)^3 = 1$. That is, $s_2^2 s_1^3$, $s_1^2 s_2^2$ are two operators of orders 4, 3 or 2, 3 respectively, whose product is of order 5, and the square of the former is invariant under both of these operators. Hence they must generate either the icosahedral group or the non-sixty group of order 120 which is isomorphic with this group. It is moreover clear that each of these two groups can be generated by two of its operators of order 5.

When $m > 1$, the six Sylow subgroups of order 5^m in G have 5^{m-1} common operators, and the corresponding quotient group has six Sylow subgroups of order 5 and is generated by them. In fact, if a group has exactly $p + 1$ Sylow subgroups of order p^m and is generated by them, these subgroups have p^{m-1} common operators which form an invariant subgroup, and the corresponding quotient group involves exactly $p + 1$ Sylow subgroups of order p and is generated by them. The preceding results clearly establish the theorem: *If a group involves exactly six Sylow subgroups of order* 5^m, *these subgroups generate a group whose order is either* $12 . 5^m$ *or* $24 . 5^m$.

UNIVERSITY OF ILLINOIS.